and show how contextual and score-based algorithms are more dynamic than criteria-based and singular algorithms. In future work, we intend to adapt score-based algorithm by analyzing the risk factors and evaluate a threshold score as confidence level above which score the PE can grant the access to a resource. To make our proposed model more dynamic, past access history to objects will be considered as a factor in activity decision making which is referred in contextual algorithm of ZTA [29].

5 CONCLUSION AND FUTURE WORK

In IoT-based connected and smart CPS, activities are inseparable part from the process of automation, and require run-time access control to allow of deny a requested activity in a system. We envision an **active** security model focusing on the activity-centric access control for smart collaborative ecosystems. The proposed ACAC model shows how current or preceding activities constraint the initiation of a new activity along with considering few other parameters such as authorizations, obligations and conditions. In this paper, we discuss the distinctions between ACAC and other related access control models. We highlight the factors for why these models are not fit for the systems with wide-range of connected IoT-based smart devices and activities. We present preliminary thoughts on model components, states of an activity and show a hierarchical structure for family of models ($ACAC_0$, $ACAC_1$, $ACAC_2$, and $ACAC_3$) that adds the significant supporting properties gradually to strengthen the model. We briefly discuss how Zero Trust tenets are supported by ACAC model.

For future work, we will develop formal operational and administrative models, policy language, and enforcement architectures for ACAC, as elaborated Gupta and Sandhu [17]. To support ZTA, we will accommodate the zero trust tenets and trust algorithms by analyzing risks present in the system. We also aim to build a self-adaptive and AI-driven ACAC model that will not need explicit policy definition for each access. AI-driven policy mining from activity logs will make the activity-centric control decision automated for connected smart CPS.

ACKNOWLEDGEMENT

This research is partially supported by NSF CREST Center Grant HRD-1736209 at UTSA, and by the NSF Grant 2025682 at TTU.

REFERENCES

[1] Safwa Ameer, James Benson, and Ravi Sandhu. 2020. The EGRBAC Model for Smart Home IoT. In *IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI)*. 457–462.
[2] Safwa Ameer and Ravi Sandhu. 2021. The HABAC Model for Smart Home IoT and Comparison to EGRBAC. In *ACM Workshop on Secure and Trustworthy Cyber-Physical Systems*. 39–48.
[3] Smriti Bhatt, Thanh Kim Pham, Maanak Gupta, James Benson, Jaehong Park, and Ravi Sandhu. 2021. Attribute-Based Access Control for AWS Internet of Things and Secure Industries of the Future. *IEEE Access* 9 (2021), 107200–107223.
[4] Smriti Bhatt and Ravi Sandhu. 2020. ABAC-CC: Attribute-based access control and communication control for internet of things. In *ACM SACMAT*. 203–212.
[5] Glen Cathey, J. Benson, M. Gupta, and R. Sandhu. 2021. Edge Centric Secure Data Sharing with Digital Twins in Smart Ecosystems. In *IEEE TPS-ISA*.
[6] Shehzad Ashraf Chaudhry et al. 2020. A secure and reliable device access control scheme for IoT based sensor cloud systems. *IEEE Access* 8 (2020), 139244–139254.
[7] Shehzad Ashraf Chaudhry et al. 2020. Securing demand response management: A certificate-based access control in smart grid edge computing infrastructure. *IEEE Access* 8 (2020), 101235–101243.
[8] Pietro Colombo, Elena Ferrari, and Engin Deniz Tümer. 2021. Regulating data sharing across MQTT environments. *JNCA* 174 (2021), 102907.
[9] Ashok Kumar Das et al. 2019. Provably secure ECC-based device access control and key agreement protocol for IoT environment. *IEEE Access* 7 (2019), 55382–55397.
[10] Deborah D Downs et al. 1985. Issues in discretionary access control. In *IEEE Symposium on Security and Privacy*. 208–208.
[11] Yanfang Fan, Zhen Han, Jiqiang Liu, and Yong Zhao. 2009. A mandatory access control model with enhanced flexibility. In *IEEE international conference on multimedia information networking and security*, Vol. 1. 120–124.
[12] Deepti Gupta et al. 2020. Access control model for Google cloud IoT. In *IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*. 198–208.
[13] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal. 2020. Security and privacy in smart farming: Challenges and opportunities. *IEEE Access* 8 (2020), 34564–34584.
[14] Maanak Gupta, Feras M Awaysheh, and others. 2020. An Attribute-Based Access Control for Cloud Enabled Industrial Smart Vehicles. *IEEE Transactions on Industrial Informatics* 17, 6 (2020), 4288–4297.
[15] Maanak Gupta and Ravi Sandhu. 2016. The $GURA_G$ Administrative Model for User and Group Attribute Assignment. In *International Conference on Network and System Security*. Springer, 318–332.
[16] Maanak Gupta and Ravi Sandhu. 2018. Authorization framework for secure cloud assisted connected cars and vehicular internet of things. In *ACM SACMAT*. 193–204.
[17] Maanak Gupta and Ravi Sandhu. 2021. Towards Activity-Centric Access Control for Smart Collaborative Ecosystems. In *ACM SACMAT*. 155–164.
[18] Maanak Gupta, Ravi Sandhu, Tanjila Mawla, and James Benson. 2022. Reachability analysis for attributes in ABAC with group hierarchy. *IEEE Transactions on Dependable and Secure Computing* (2022).
[19] Sergio Gusmeroli, Salvatore Piccione, and Domenico Rotondi. 2013. A capability-based security approach to manage access control in the internet of things. *Mathematical and Computer Modelling* 58, 5-6 (2013), 1189–1205.
[20] Weijia He, Maximilian Golla, et al. 2018. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). In *USENIX Security*. 255–272.
[21] Vincent C Hu, D Richard Kuhn, David F Ferraiolo, and Jeffrey Voas. 2015. Attribute-based access control. *IEEE Computer* 48, 2 (2015), 85–88.
[22] Xin Jin, Ram Krishnan, and Ravi Sandhu. 2012. A unified attribute-based access control model covering DAC, MAC and RBAC. In *IFIP Annual Conference on Data and Applications Security and Privacy*. Springer, 41–55.
[23] Savith Kandala, Ravi Sandhu, and Venkata Bhamidipati. 2011. An attribute based framework for risk-adaptive access control models. In *IEEE International Conference on Availability, Reliability and Security*. 236–241.
[24] Ji Eun Kim et al. 2012. Seamless integration of heterogeneous devices and access control in smart homes. In *International Conference on Intelligent Environments*. 206–213.
[25] Javier Lopez and Juan E Rubio. 2018. Access control for cyber-physical systems interconnected to the cloud. *Computer Networks* 134 (2018), 46–54.
[26] Jaehong Park and Ravi Sandhu. 2004. The $UCON_{ABC}$ usage control model. *ACM transactions on information and system security (TISSEC)* 7, 1 (2004), 128–174.
[27] Jaehong Park, Ravi Sandhu, and Yuan Cheng. 2011. ACON: Activity-centric access control for social computing. In *IEEE ARES*. 242–247.
[28] Jaehong Park, Ravi Sandhu, Maanak Gupta, and Smriti Bhatt. 2021. Activity Control Design Principles: Next Generation Access Control for Smart and Collaborative Systems. *IEEE Access* 9 (2021), 151004–151022.
[29] Scott Rose, Oliver Borchert, Stu Mitchell, and Sean Connelly. 2020. Zero Trust Architecture. *National Institute of Standards and Technology* (2020).
[30] RS Sandhu, EJ Coyne, HL Feinstein, and CE Youman Role-Based. 2013. Access control models. *IEEE computer* 29, 2 (2013), 38–47.
[31] Ravi Sandhu and Jaehong Park. 2003. Usage control: A vision for next generation access control. In *International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security*. Springer, 17–31.
[32] Ravi S Sandhu and Pierangela Samarati. 1994. Access control: principle and practice. *IEEE communications magazine* 32, 9 (1994), 40–48.
[33] Roei Schuster, Vitaly Shmatikov, and Eran Tromer. 2018. Situational access control in the internet of things. In *ACM SIGSAC Conference on Computer and Communications Security*. 1056–1073.
[34] Abhijeet Thakare, Lee, et al. 2020. PARBAC: priority-attribute-based RBAC model for azure IoT cloud. *IEEE Internet of Things Journal* 7, 4 (2020), 2890–2900.
[35] Roshan K Thomas and Ravi S Sandhu. 1994. Conceptual foundations for a model of task-based authorizations. In *Proceedings of IEEE Computer Security Foundations Workshop VII*. 66–79.
[36] Roshan K Thomas and Ravi S Sandhu. 1998. Task-based authorization controls (TBAC): A family of models for active and enterprise-oriented authorization management. In *Database security XI*. Springer, 166–181.
[37] Ronghua Xu, Yu Chen, Erik Blasch, and Genshe Chen. 2018. A federated capability-based access control mechanism for internet of things (iots). In *Sensors and Systems for Space Applications XI*, Vol. 10641. International Society for Optics and Photonics, 106410U.